REMARKS

Claims 1-30 are pending in the present application. Claims 1-34 were presented for examination. Claims 31-34 were cancelled by amendment.

In the office action mailed January 27, 2006 (the "Office Action"), the Examiner rejected claims 1-35 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,449,719 to Baker *et al.* (the "Baker patent") in view of U.S. Patent No. 6,810,525 to Safadi *et al.* (the "Safadi patent").

The Examiner's rejection of claims 31-34 under 35 U.S.C. 103(a) is now moot in light of the cancellation of these claims.

The Baker patent discloses a process to encrypt a pay-on-demand data stream that is provided to a client machine over a network, such as the Internet. The data stream cannot be stored on a client machine for future playback or re-transmission, thereby protecting copyrighted works from being easily disseminated from the client machine. The data stream is encrypted when transmitted from the server to the client machine, which includes client software for decrypting the encrypted data. *See* col. 4, lines 17-29. Access to the encrypted data, however, is controlled by using a different encryption key for decryption every time the data is accessed. That is, a different encryption key is created so the data cannot be accessed at a later time even if the data is saved to disk on the client machine. *See* col. 4, lines 31-36.

When a connection between the client machine and the server are initially created, user information, a requested URI, and a token are provided to the server. If the information indicates that the client machine is authorized to receive the data, a set of encryption keys are negotiated between the client machine and the server. Using the set of encryption keys, the server encrypts the stream of data as it is being transmitted and the client machine decrypts the same data as it is received. *See* col. 4, line 64-col. 5, line 5 and col. 5, line 66-col. 6, line 14.

A token is created by a transaction server that is contacted by the client machine prior to connecting to the server. The transaction server generates the token in response to verification of the user information provided from the client machine. As previously discussed, the token and other user information is transmitted to the server by the client machine to receive the encrypted data stream.

The Safadi patent has been cited by the Examiner as teaching the limitations of generating a token, initiating a request to open a computer resource, verifying whether the user has sufficient credit, decrypting and opening the requested computer resource, monitoring usage, and providing notification. *See* the Office Action at pages 4 and 5.

Claims 1, 11, 19, and 27 are patentable over the Baker patent in view of the Safadi patent because the combined teachings of the references do not teach or suggest the combination of limitations recited by the respective claims.

For example, with reference to claim 1, the combined teachings fail to disclose a method for providing access to computer resources that includes decrypting at the computer system a token and authenticating a user of the computer system using authentication information stored in the token. As previously discussed, the Baker patent describes a process where the client machine receives a token from the transaction server and provides the same token to the server when a connection is created and request for the data to be transmitted is made. The Safadi patent, as discussed in detail in the remarks of the previously submitted response, describes a system where a subscriber terminal 16 securely forwards an encrypted entitlement token to a server 18 for fulfillment. The subscriber terminal 16 does not decrypt the entitlement token.

The Examiner argues that the encrypted token described in the Safadi patent combined with the provision of a token by the client machine to the server described in the Baker patent teaches decrypting an encrypted token at the computer system. However, at best, the combination of the Baker and Safadi patent teaches providing an encrypted token to a server from which data is provided, and not decrypting an encrypted token at the computer system (i.e., subscriber terminal or client machine). Provision of the token from the client machine and the subscriber terminal 16 to the server is the same process in both the Baker patent and the Safadi patent, the distinction being that in one case the token is expressly described as being encrypted (i.e., the Safadi patent) and in the other case, the token is not described as being encrypted (i.e., the Baker patent). Changing the token described in the Baker patent to be an encrypted token, based on the teachings of the Safadi patent, merely creates the same process as described in the Safadi patent, which is to provide the token (now encrypted) from the client machine to the server for provision of the stream of encrypted data. Moreover, as described in the Baker patent,

"it is not desirable for the client to have any way of determining if the token is valid or not." *See* col. 4, lines 46-48. Although describing the expiration date of the token, the description suggests that it is not desirable for information included in the token to be accessible at the client machine. Consequently, based on the teachings of the Baker patent, it is unlikely that decryption of an encrypted token at the client machine is desirable.

In contrast, as described for an embodiment in the present application, an encrypted token provided to the client computer systems 204, 206 by the server 202 is decrypted at the client computer system 204, 206. Decryption of the token at the client computer system 204, 206 allows for access to computer resources in both broken-connection and continuous-connection environments. In a broken-connection environment, the computer resources are accessed without connecting to the server. In the system described in the Baker patent, for the encrypted data to be accessible, a continuous connection is required. Moreover, the Baker patent suggests that access to the encrypted data after the connection between the client machine and the server is broken is undesirable. *See* col. 4, lines 31-36.

Claims 11, 19, and 27 recite limitations similar to that previously discussed with reference to claim 1. For example, claim 11 recites a method for providing access to computer resources on a computer system that includes, among other things, decrypting at the client system the token in response to a request to initiate execution of one of the computer resources. Claim 19 recites a method for providing access to computer resources on a computer system that includes decrypting at the client system the token and authenticating a user of the client computer system. Claim 27 recites a client system for providing access to computer resources having a remote application manager component operable to decrypt at the client system the encrypted user information. As previously discussed, the combined teachings of the Baker patent and the Safadi patent fails to teach or suggest at least the limitation of decrypting an encrypted token at the client computer system.

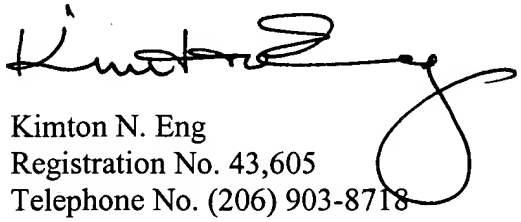
For the foregoing reasons, claims 1, 11, 19, and 27 are patentable over the Baker patent in view of the Safadi patent. Claims 2-10, which depend from claim 1, claims 12-18, which depend from claim 11, claims 20-26, which depend from claim 19, and claims 28-30, which depend from claim 27, are similarly patentable because of their dependency from a

respective allowable base claim. Therefore, the rejection of claims 1-30 under 35 U.S.C. 103(a) should be withdrawn.

All of the claims pending in the present application are in condition for allowance. Favorable consideration and a timely Notice of Allowance are earnestly solicited.

Respectfully submitted,

DORSEY & WHITNEY LLP



Kimton N. Eng
Registration No. 43,605
Telephone No. (206) 903-8718

KNE:ajs

Enclosures:
Postcard
Check
Fee Transmittal Sheet (+ copy)

DORSEY & WHITNEY LLP
1420 Fifth Avenue, Suite 3400
Seattle, WA 98101-4010
(206) 903-8800 (telephone)
(206) 903-8820 (fax)

h:\ip\clients\micron technology\700\500767.01\500767.01 amendment 2.doc